I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

An Economic Argument for Electronic Privacy

JAKE SPRATT*

Abstract: This Article proposes an economic framework with which to analyze the U.S.'s electronic privacy laws in the context of international privacy standards. A key assumption is that electronic privacy generally exists in tension with the speed and convenience of e-commerce: if privacy protections are too strong, e-commerce will suffer. At the same time, however, this Article shows that consumers expect a certain basic level of privacy when they conduct electronic transactions. A government that fails to provide this certain level of privacy effectively weakens the e-commerce industry. This Article concludes the United States has failed to guarantee sufficient privacy protections and that, by learning from the E.U. and Canada, the U.S. can increase both personal privacy and the effectiveness of e-commerce by enacting comprehensive electronic privacy laws.

INTRODUCTION

The technological revolution and the emergence of mass communications have irreversibly changed the face of personal privacy. Although traditional threats to privacy still exist, such as involuntary disclosure of personal information in newsprint, "our privacy is peculiarly menaced by the evolution of modern society, with its burgeoning technologies of surveillance and inquiry."[1] There is no

* Associate, Sherman & Howard, LLC, Denver, Colorado. J.D., University of Denver Sturm College of Law, M.S., Economics, Oregon State University, B.A., Economics, Washington State University. The author thanks Dennis Hirsch, J. Zachary Courson, John Soma, and the very capable editors of the *I/S Journal of Law and Policy for the Information Society* for their helpful comments on this Article.

[1] James Q. Whitman, The Two Western Cultures of Privacy: Dignity Versus Liberty, 113 YALE L.J. 1151, 1153 (2004).

greater example of these "burgeoning technologies" than the World Wide Web, which enables tens of millions of people across the world to freely exchange massive amounts of information almost instantly.[2] While this incredible advancement has enabled explosive economic growth, the technology has not come without a price.

The Internet's rapid growth in scale, scope, and usage has led to a dramatic increase in the number of public disclosures of personal information. "[E]-commerce companies often require physical and email addresses, phone numbers, zip codes, birthdays, gender identification, and other miscellaneous information *merely to set up an online account.*" Many of these disclosures are not necessary to complete the desired transactions,[3] yet most users voluntarily relinquish their private information without a second thought.[4]

With all of this information flying about, one wonders what safeguards are in place to protect the personal privacy of Internet users. Most large websites have adopted and published some sort of a privacy policy, whether through a separate hyperlink or embedded in a "Terms of Use" agreement.[5] In the United States, however, there is no law requiring websites to adopt and post a privacy policy,[6] let alone

---

[2] James Q. Whitman, The Two Western Cultures of Privacy: Dignity Versus Liberty, 113 YALE L.J. 1151, 1153 (2004).

[3] *See id.* at 559. For example, the popular search engine and email portal Yahoo! requires each user to disclose his or her full name, gender, birth date, and zip code before establishing an account. Yahoo! Registration, https://edit.yahoo.com/registration?.intl=us&new=1&.done=http%3A//mail.yahoo.com&.src=ym (last visited Mar. 8, 2011). It is unclear why Yahoo! would require the gender and birth date of a potential member simply to set up an email account. Indeed, another popular email portal, Google, does not require this information at all while providing essentially the same service. *See* Google Accounts, https://www.google.com/accounts/NewAccount?continue=http%3A%2F%2Fwww.google.com%2F&hl=en (last visited Mar. 8, 2011).

[4] *See* Ciocchetti, *supra* note 3, at 561-62 (arguing that the "just click submit" phenomenon is largely motivated by electronic consumers' "must, rush, and trust tendencies").

[5] A 2007 survey of the top twenty-five most visited websites revealed that every one of those sites posted a privacy policy statement. Ciocchetti, *supra* note 3, at 599. However, only seventeen of those sites conspicuously posted a policy on the site's homepage. *Id.* The remaining 8 sites either posted their policies on a secondary page or posted a link on the homepage that was difficult to identify. *Id.*

[6] Ciocchetti, *supra* note 3, at 610-11; *see also infra* Part II.C for a discussion of U.S. electronic privacy law.

a law requiring websites to adopt certain provisions *within* a policy.[7] While other countries have adopted comprehensive electronic privacy laws, the United States seems content to let the free market regulate privacy. In most instances, therefore, website operators need only follow the privacy protections that they themselves have written and chosen to adopt. With the fox left guarding the henhouse, one begins to wonder, *quis custodiet ipsos custodes?*[8]

This Article analyzes United States privacy law as it pertains to electronic transactions (or "e-commerce") and the use of electronically stored personally identifiable information ("PII"). Unlike many other countries, the United States does not have a single overarching electronic privacy law. Many commentators have argued that the U.S. should adopt a comprehensive set of privacy protections similar to those adopted in the European Union and Canada. Against that backdrop, this Article examines the laws of the E.U. and Canada as alternatives to the U.S. system. Rather than provide yet another survey of the existing laws,[9] however, this Article posits the question, "Which system of privacy laws is best?"

Of course, if privacy laws operated in a vacuum, that question would be very easy to answer: the country with the most protections wins. As with most questions of law and public policy, however, the answer is not that simple. Speed and convenience are central to the allure of electronic commerce, and privacy protections may undermine the ease with which consumers conduct online transactions.[10] Thus, any regime that attempts to tackle electronic privacy must be careful not to quash the very speed and convenience that is the lifeblood of e-commerce. The question then becomes,

---

[7] The United States, for example, does not require website operators to adopt a privacy policy. *See infra* Part II.B.

[8] "Who will watch the watchmen?"

[9] There are many excellent sources that summarize the E.U., U.S., and Canadian privacy law in much greater detail than is afforded here. *E.g.*, Avner Levin & Mary Jo Nicholson, *Privacy Law in the United States, the E.U. and Canada: The Allure of the Middle Ground*, 2 OTTAWA L. & TECH. J. 357 (2005); Virginia Boyd, *Financial Privacy in the United States and the European Union: A Path to Transatlantic Regulatory Harmonization*, 24 BERKELEY J. INT'L L. 939 (2006) (comparing and contrasting U.S. and E.U. privacy laws as they relate to financial data). This Article provides only a cursory review of these laws in order to introduce (and justify) a new economic model for analyzing privacy laws in Part III.

[10] Julia M. Fromholz, *Data Privacy: The European Union Data Privacy Directive*, 15 BERKELEY TECH. L.J. 461, 465 (2000).

"What is the optimal *balance* between privacy protections and the efficiency of e-commerce?"

To attempt to answer *that* question, this Article constructs an economic model that reflects the relationship between privacy protections and the speed and convenience of e-commerce. The model begins by asserting three relatively uncontroversial axioms:

1. People value both privacy and efficiency in e-commerce.[11]

2. Privacy protections and efficiency are in tension, which causes a tradeoff between the two.

3. At some point, people will not conduct electronic transactions if they feel their private information is not adequately protected.

From these statements, an economic model is constructed to emulate the relationship between privacy protection laws and the efficiency of electronic commerce. The model is used to show that consumers expect a certain basic level of privacy when they conduct electronic transactions. A government that fails to provide this certain level of privacy effectively weakens the e-commerce industry. Finally, this Article argues that the United States has failed to guarantee sufficient privacy protections and that, by learning from the E.U. and Canada, the U.S. can increase *both* personal privacy and the efficiency of e-commerce by enacting comprehensive electronic privacy laws.

Part I of this Article contextualizes the privacy-efficiency tradeoff by surveying electronic privacy laws in three governing bodies—the United States, the European Union, and Canada. Part II constructs a simple economic framework to model the tradeoff between privacy and efficiency, and uses the discussion from Part I to map the United States, the E.U., and Canada's electronic privacy laws onto a privacy–efficiency "tradeoff frontier." Part II also argues that without a basic level of privacy protection—a "tradeoff threshold"—some consumers will *reduce* the number of transactions they undertake, meaning that the tradeoff is not absolute. Part III then argues that the United States' laws currently exist below the "tradeoff threshold," meaning that the U.S. could increase *both* privacy and efficiency by enacting

[11] "Privacy" and "efficiency" are somewhat amorphous terms. Part III specifically defines these terms as they are used in this paper and the model within it. For now, the general understanding of each word will suffice.

comprehensive legislation. Finally, Part IV explains why the United States' current "free market" approach is ill suited for electronic privacy, and suggests three modest steps the U.S. should take to increase both privacy protections and the efficiency of electronic commerce.

I. A (BRIEF) SURVEY OF 21ST CENTURY PRIVACY LAW

In today's global economy, "it is virtually meaningless to talk of national privacy law."[12] Instead, it is best to examine electronic privacy laws in the context of international transactions. The free exchange of information is essential to international commerce, and it is not uncommon for companies to send data across several continents to complete a single transaction.[13] At the same time, individual countries continue to impose their own rules on data transactions originating from, or destined to, their jurisdictions—rules that unavoidably extend to commercial (and often personal) entities in other countries. Thus, any inquiry into a single country's electronic privacy laws necessarily involves an examination of how those laws interact with other governing bodies. As one commentator summarized the situation:

> The ubiquity of computers and the growth of networks have made the collection, analysis, and dissemination of personal data inexpensive and easy. This growth has also led to a heightened concern about the level of protection afforded to personal data. . . . Some countries seeking to protect the privacy of their citizens' data have done so in ways that extend the reach of their data privacy laws into other countries. Conflict over such reach is virtually inevitable and, if serious, will likely impede the growth of worldwide electronic commerce.[14]

The following sections compare privacy laws in the E.U., the U.S., and Canada, with a focus on electronically-stored PII. To facilitate the comparison, the "lifespan" of electronic information is partitioned into four categories: collection, use, dissemination, and redress.

---

[12] Boyd, *supra* note 10, at 939.

[13] See id.

[14] Fromholz, *supra* note 11, at 461.

1. COLLECTION

"Collection" refers to the circumstances under which electronic entities gather and record PII. Almost all major websites collect PII both actively and passively.[15] Common concerns raised with the collection of PII include notice and consent requirements, "opt in" versus "opt out" choices, and the level of transparency entities must adopt.

2. USE

By comparison, "use" considers what things electronic entities can do with PII once it is collected. An online entity may use PII for any number of reasons, including for internal research, for directed marketing, or to increase user convenience (for example, remembering user login information).[16] Common "use" issues include how an online entity can process personal information (including "profile building"), solicitations, and directed marketing.

3. DISSEMINATION

"Dissemination," in contrast with "use," relates to *if*, *when*, and *how* a collecting entity can share PII with third parties. The sale of electronic profiles to marketing companies is a particularly touchy concern raised within dissemination." Online entities can quickly and easily generate revenue by selling PII to third parties, who then use the information to construct consumer "profiles."[17] The nature of electronic data makes PII virtually irretrievable once an entity has disclosed it to an outside source.[18]

---

[15] A 2007 survey revealed that each of the top twenty-five most visited websites collected user information both actively and passively. Ciocchetti, *supra* note 3, at 601.

[16] To be sure, many of the ways online entities use PII appear highly agreeable. For example, the popular video rental site Netflix.com asks users to rate recently viewed movies on a scale of 1-5. The site stores a particular user's ratings and looks for other users with similar tastes. Netflix then recommends additional titles based on the ratings of other users with similar preferences. Thus, the site's collection and use of PII allows the company to distinguish itself from traditional "walk in" video stores by offering customized recommendations specifically tailored from a given user's preference profile.

[17] Ciocchetti, *supra* note 3, at 576.

[18] *Id.* at 579-81.

4. REDRESS

Finally, "redress" captures the available remedies (if any) a governing entity affords consumers. A remedy might be a right to pursue a private action against a privacy violator, the right to file a complaint with an administrative body, or the right to access and correct any stored PII. The availability of redress protects privacy by allowing consumers to redact false information and by deterring those who would wrongly collect, use, or disseminate PII.

The following sections analyze the protections afforded by the E.U., the U.S., and Canada in each of these four stages. Relevant comparisons between the three governing entities are then drawn. In the end, the E.U. emerges as the most protective of PII, while the U.S. affords the least amount of protection. Canada, both federally and provincially, lies somewhere between the two.

A. THE EUROPEAN UNION

Much of the difference in privacy law between the U.S. and E.U. can be attributed to the cultural differences between the two entities.[19] In most of continental Europe, personal privacy is considered a fundamental human right,[20] similar to the right to free speech in the United States. To Europeans, the right to control the public dissemination of private information is a matter of human dignity; the unwilling disclosure of personal information is both distasteful and deeply offensive.[21] As a consequence, Europeans have placed a greater

---

[19] *See generally* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L. J. 1151 (2004). Professor Whitman argues that the current privacy law in the E.U. and U.S. is the product of cultural differences, which, in turn, are a product of historical social norms. He states, "Privacy law is not the product of logic . . . It is the product of local social anxieties and local ideals. In the United States those anxieties and ideals focus . . . around the ambition 'to secure the blessings of liberty,' while on the Continent they focus on the ambition to guarantee . . . everyone's 'honor.'" *Id.* at 1219-20.

[20] Fromholz, *supra* note 11, at 462. Indeed, Directive 95/46/EC repeatedly refers to the right to privacy as one of the "fundamental rights and freedoms" held by all people. *E.g.*, Council Directive 95/46/EC, 1995 O.J. (L281) 31, Preamble (2), (10), (11).

[21] Whitman, *supra* note 1, at 1192-94. Professor Whitman does not argue that Europeans are hermetical by nature (that is, that Europeans are necessarily resistant to public life). Rather, Professor Whitman claims Europeans expect a certain degree of *control* over the public dissemination of their private affairs. He illustrates this point using a particularly revealing (excuse the pun) example: public nudity. In many regions in Europe, it is common to see a fully nude person sunbathing in a public park. While a nude sunbather has clearly consented to public viewing of his or her body, it would be considered a

emphasis on protecting the individual's "dignity," through greater restrictions on electronic data, than on protecting the efficiency of e-commerce.[22] Consistent with this view, the European Union has adopted regulations that significantly restrict how entities can collect, use, and disseminate electronically stored PII.

1. DIRECTIVE 95/46/EC[23]

In 1995, the European Commission enacted a comprehensive directive designed to "harmonize data privacy laws among the fifteen member states" by setting a "minimum level of [privacy] protection" by which all member states were to abide.[24] The legislation, commonly referred to as the "Data Privacy Directive," explicitly balances the need to "mak[e] the processing and exchange of such data considerably easier" among member states, with the need to "respect [the] fundamental rights and freedoms, notably the right to privacy," of individual people.[25] The Directive accomplishes these objectives by significantly limiting the collection, use, and dissemination of PII. The Directive also creates several avenues of redress available to PII subjects whose privacy has been violated.

a. COLLECTION

With very few exceptions, the Data Privacy Directive prohibits the collection of PII from any user who has not "unambiguously given his

---

violation of personal privacy if a photographer were to capture and disseminate images of the publicly nude person. "The difference," Professor Whitman explains, "is not that Europeans refuse to be seen nude, but that they insist that they want to be the ones who should determine *when* and under *what circumstances* they will be seen nude." *Id.* at 1201 (emphasis added). To most Europeans, involuntary public dissemination of one's nude image would violate the right to control one's public life, even if that image was captured in a decidedly public setting. *Id.*

[22] *See id.*, at 1192.

[23] Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter "Directive 95/46/EC," or "Data Privacy Directive"].

[24] Fromholz, *supra* note 11, at 468.

[25] Directive 95/46/EC, at Preamble (2), (4).

consent" to the collection.[26] The Directive defines "consent" as "any *freely given specific* and *informed* indication of [a data subject's] wishes by which the data subject signifies his agreement to personal data relating to him being processed."[27]

Against this strong language, the Directive enumerates limited exceptions to the consent requirement. For example, an entity may collect PII without a data subject's consent if collection is "necessary for compliance with a legal obligation"[28] or for "performance of a contract to which the data subject is party."[29] Additionally, the Directive contains exemptions pertaining to national security,[30] "legitimate" government interests,[31] or when necessary "to protect the vital interests of the data subject."[32]

b. USE

The Data Privacy Directive broadly defines "processing of personal data" to mean any action involving the "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, . . . [or] erasure or destruction" of PII.[33] Thus, the restrictions that apply to the collection of PII also apply to use and dissemination.[34] Most notably, online entities must obtain "unambiguous consent" before they "use" PII.

The Directive restricts the use of PII in other ways. For example, all data involving personally identifiable information must be

---

[26] *Id.* at ch. II, § II, art. 7, cl. (a).

[27] *Id.* at ch. I, art. 2, cl. (h) (emphasis added).

[28] *Id.* at ch. II, § II, art. 7, cl. (c).

[29] *Id.* at ch. II, § II, art. 7, cl. (b).

[30] *Id.* at ch. II, § II, art. 7, cl. (e).

[31] Directive 95/46/EC, *supra* note 24, at ch. II, § II, art. 7, cl. (f).

[32] *Id.* at ch. II, § II, art. 7, cl. (d).

[33] *Id.* at ch. I, art. 2, cl. (b).

[34] The "unambiguous consent" language in chapter II, section II, article 7 applies to *all* "processing of personal data," a term that, as shown above, applies to use as well as dissemination.

processed "fairly and lawfully."[35] Once PII is collected, online entities can only use the data in ways that are compatible with the "specified, explicit and legitimate purposes" for which the information was originally collected.[36] Finally, the Directive calls on member states to "implement appropriate technical and organizational measures to protect personal data against . . . loss, alteration, unauthorized disclosure or access."[37] Online entities operating within a member state must then abide by the state's "technical and organizational measures" if the entity wishes to use PII.

c. DISSEMINATION

The Directive's restrictions on third-party transfers are perhaps the most restrictive in the world, and pose a significant threat to international transactions.[38] *Within* the member states, an entity may not transfer PII to another entity without the informed, unambiguous consent of a data subject.[39] This restriction comports with the Directive's other limits on collection and use. However, it is the restriction on data transfers *outside* of the E.U. that raises serious concerns.

Article 25 prohibits "the transfer to a third country of personal data" except where "the third country in question ensures an *adequate level of protection.*"[40] The Directive leaves the phrase "adequate level of protection" notably undefined,[41] offering as guidance only that "[t]he adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances."[42] While the exact contours of "adequate protection" remain unclear, what is clear

---

[35] Directive 95/46/EC, *supra* note 24, at ch. II, § I, art. 6, cl. 1(a).

[36] *Id.* at ch. II, § I, art. 6, cl. 1(b).

[37] *Id.* at ch. II, § VIII, art. 17, cl. 1.

[38] *See* Fromholz, *supra* note 11, at 474.

[39] *See* Directive 95/46/EC, *supra* note 24, at ch. I, art. 2, cl. (b), (h), & ch. II § II, art. 7, cl. (a).

[40] *Id.* at ch. IV, art. 25, cl. 1 (emphasis added).

[41] Fromholz, *supra* note 11, at 469.

[42] Directive 95/46/EC, *supra* note 24, at ch. IV, art. 25, cl. 2.

is that many of the world's countries—including the U.S.—do *not* pass the test.[43]

The practical impact of this provision cannot be overstated. "Without a resolution the stand-off [between the E.U. and non-compliant third countries] could result in an extreme hindrance to global trade."[44] The free flow of information is critical to commerce, and the Directive places a significant restriction on that flow. As one commentator noted, "strictly implemented, the Directive could prohibit [even] mundane transactions such as the transfer of data from the European subsidiary of a multinational company to its American headquarters."[45]

There are a few provisions that lessen the Directive's otherwise draconian restrictions on data transfers and soften the potential effect on international commerce. A third country may, for example, negotiate an agreement with the Council whereby the Council uniformly declares the country "safe" for data transfers. [46] The Directive also outlines limited exceptions in which personal data may be sent from the E.U. to an "inadequate" third country,[47] such as when the transfer is needed to satisfy a legal obligation[48] or to protect an "important public interest."[49] Outside of these limited situations, however, data processing entities in the E.U. *cannot* transfer PII data to any third country that does not meet the Council's definition of "adequate protection."

---

[43] Boyd, *supra* note 10, at 940. Ms. Boyd notes that although "[v]arying degrees of privacy legislation exist in different sectors of the U.S. economy . . . the European Union has not found that the overall level of protection in the United States meets the European standards." *Id.*

[44] Kevin Bloss, Note, *Raising or Razing the e-Curtain?: The E.U. Directive on the Protection of Personal Data*, 9 MINN. J. GLOBAL TRADE 645, 646 (2000).

[45] Fromholz, *supra* note 11, at 474.

[46] Directive 95/46/EC, *supra* note 24, at ch. IV, art. 25, cl. 6.

[47] For a full list of exceptions, *see id.* at ch. IV, art. 26.

[48] *Id.* at ch. IV, art. 26, cl. 1 (b), 1 (d).

[49] *Id.* at ch. IV, art. 26, cl.1 (d).

d. REDRESS

The Data Privacy Directive provides several avenues of relief for a person whose PII has been mishandled. First, Article 22 requires that "Member States shall provide for the right of every person to a judicial remedy for *any* breach of the rights guaranteed him."[50] Second, Article 23 provides that "any person who has suffered damage as a result of an unlawful processing operation . . . is entitled to receive compensation from the controller[51] for the damage suffered."[52]

Third, the Directive endows data subjects with a broad right to access their PII once it has been collected and stored. Article 12 grants a data subject the right to know "whether or not data relating to him are being processed," the purpose behind any such processing, and full disclosure of the recipients of the processed data (if any).[53] Finally, data subjects have the right to correct any false information pertaining to their PII and the right to block or destroy any stored data that was collected, used, or disseminated in violation of the Directive.[54]

B. THE UNITED STATES

Unlike the European Union, the United States does not have "a single, overarching privacy law."[55] Instead, the United States employs a scattered system of threat- and industry-specific protections aimed at curbing particularized threats to privacy.[56] Commentators have described this system (in varying degrees of disparagement) as "reactive,"[57] "disjointed and piecemeal,"[58] "a patchwork quilt,"[59] and,

---

[50] *Id.*at ch. III, art. 22.

[51] The "controller" is the entity charged with "[determining] the purposes and means of the processing of personal data." *Id.* at ch. I, art. 2, cl. (d). Effectively, the controller acts as a government agency that specifies if and how an entity can process PII.

[52] Directive 95/46/EC, *supra* note 24, at ch. III, art. 23, cl. 1.

[53] *Id.* at ch. II, § V, art. 12, cl. (a).

[54] *Id.* at ch. II, § V, art. 12, cl. (b).

[55] Fromholz, *supra* note 11, at 471.

[56] For a brief and comprehensive summary of federal privacy laws in the United States, *see* Levin & Nicholson, *supra* note 10.

[57] *Id.*

perhaps most illustratively, as "a sectoral 'skyline,' with skyscrapers (high regulation) in some areas . . . and tenements (lower regulation) in others."[60]

This oblique approach to privacy protections can be at least partly attributed to how Americans view privacy itself. Unlike the E.U.,[61] "[t]he United States and its companies refuse to acknowledge personal data privacy as a fundamental human right."[62] Indeed, the U.S. Constitution "does not explicitly mention *any* right of privacy" in its articles or amendments.[63] This is not to say that Americans live completely unprotected from personal intrusions. The U.S. Supreme Court has long recognized an *implied* right of privacy in the word "liberty,"[64] which is protected by the 5th and 14th Amendments to the U.S. Constitution.[65]

---

[58] *Id.* at 361.

[59] *Id.* at 360.

[60] Boyd, *supra* note 10, at 941.

[61] The Convention for the Protection of Human Rights and Fundamental Freedoms expressly recognizes privacy as a fundamental human right. Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, Eur. Ct. H.R., *available at* http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/EnglishAnglais.pdf (last visited Feb. 12, 2011). The Data Privacy Directive incorporates by reference this right to privacy. Directive 95/46/EC, *supra* note 24, at Preamble (1).

[62] Bloss, *supra* note 45, at 650.

[63] Roe v. Wade, 410 U.S. 113, 151 (1973) (emphasis added).

[64] *Id.* ("In a line of decisions, however, going back perhaps as far as [1891], the Court has recognized that a right of personal privacy . . . does exist under the Constitution."). The Court has stopped short of providing an exhaustive (or even illustrative) list of privacy rights protected within "liberty." The Court has only identified specific instances where "liberty" protects a narrowly specified right. *See, e.g.*, Loving v. Virginia, 388 U.S. 1 (1967) (interracial marriage); Parenthood v. Casey, 505 U.S. 833 (1992) (terminate pregnancy through abortion); Lawrence v. Texas, 539 U.S. 558 (2003) (same-sex sodomy). As *Lawrence* and *Casey* attest, the implicit recognition of rights protected by the word "liberty" has resulted in some of the most contentious decisions in the U.S. Supreme Court's long history. In addition to arguments over the right to consensual same-sex sodomy (*Lawrence*) and the termination of pregnancy through abortion (*Casey*), the debate over what substantive rights are protected by "liberty" has caused the Supreme Court considerable embarrassment and has sparked a prolonged and divisive debate over the role of the courts in our tri-partite system of governance. *See* Lochner v. New York, 198 U.S. 45 (1905). The Supreme Court's post-*Lochner* reluctance to read new substantive rights into the word "liberty," such as a right to electronic privacy, is perhaps another argument in favor of uniform federal legislation (although one that far exceeds the scope of

The indirect constitutional protection is not the only reason electronic privacy laws in the U.S. have lagged behind the E.U. Traditionally, Americans have been most fearful of *government* intrusions into their personal affairs, not of corporate invasions.[66] Americans seem to treat their privacy in the commercial world "as akin to personal property . . . it may be bargained and exchanged for other rights and privileges,"[67] including certain commercial benefits. America's deeply entrenched Orwellian fear of "Big Brother,"[68] however, has produced a batch of relatively strict privacy laws that apply *exclusively* to government actors. Meanwhile, the private sector has remained largely unregulated.

For example, the Privacy Act of 1974[69] limits the federal government's ability to collect, retain, and process personal information, [70] and provides individual citizens with a right to review and have their records corrected.[71] The restrictions imposed by this act are similar in nature to the restrictions imposed by the E.U.'s Data Privacy Directive.[72] However, unlike the E.U.'s Directive, the protections in the Privacy Act of 1974 only apply to federal government agencies—*not* to private companies.

---

this paper). For an example of an argument in this vein, *see* Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space*, 82 TEX. L. REV. 1329 (2004).

[65] U.S. CONST. amends. V, XIV. The indirect and implied acknowledgement of a right to privacy (as opposed to the European Union's express recognition of privacy as a human right) provides an interesting insight into the differences in how the two governing entities treat the collection, use, and dissemination of PII.

[66] *See* Whitman, *supra* note 1, at 1161-63; *see also* Levin & Nicholson, *supra* note 10, at 359.

[67] Gail Lasprogata et al., *Regulation of Electronic Employee Monitoring: Identifying Fundamental Principle of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada*, 2004 STAN. TECH. L. REV. 4, 6 (2004).

[68] "It is the rare privacy advocate who resists citing Orwell when describing these dangers." Whitman, *supra* note 1, at 1153.

[69] 5 U.S.C. § 552a.

[70] *Id.* § 552a(b), (e-f).

[71] *Id.* § 552a(d).

[72] *See supra*, Part II.A.

There are several other statutes in the U.S. that protect against unwarranted government intrusion into personal privacy, statutes that, by definition, do not apply to private actors.[73] These statutes generally protect against unwarranted "search and seizure" in electronic fora.[74] Fear of government surveillance, however, does not appear to significantly affect the scale or scope of e-commerce. Thus, these statutes are largely irrelevant for purposes of this Article, and they are not discussed in any detail.

Because the United States does not operate under a single, unified privacy law, it is difficult to examine the U.S. using the "collection, use, dissemination, and redress" framework. Instead, the following subsections analyze the various industry-specific laws in the U.S. Consistent with the scope of this Article, only those laws that significantly affect some area of e-commerce and electronic privacy are discussed. Other legislation, while relevant to American privacy law in general, is not discussed here.[75]

1. THE FINANCIAL MODERNIZATION ACT (A.K.A. GRAMM-LEACH BLILEY ACT)[76]

The Gramm-Leach Bliley Act (GLBA) is one of the most important (and restrictive) privacy laws in the United States. The GLBA applies to the use of PII by banks and other financial institutions.[77] The Act requires financial institutions to adopt a privacy policy that explains how the institution collects, uses, and disseminates PII.[78] While the

---

[73] *E.g.*, The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 (1986) (restricting warrantless electronic surveillance during criminal investigation); The Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g (1974) (limiting disclosure of student information by federally-funded schools); The Driver's Privacy Protection Act, 18 U.S.C. 2721 (1994) (restricting disclosure of private information by state motor vehicle offices).

[74] *See* The Electronic Communications Privacy Act of 1986, *supra* note 74; FERPA, *supra* note 74; The Drier's Privacy Protection Act, *supra* note 74.

[75] For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulates the use of personal health information by health professionals. The law does not appear to have a significant impact on electronic commerce outside of intra-health care entity recordkeeping. Accordingly, it is not discussed here.

[76] 15 U.S.C. §§ 6801-6809 (1999).

[77] *See id.*

[78] *See id.* § 6803.

Act requires the adoption of such a policy, it does not stipulate what *terms* are to be included within the policy. Thus, the Act "fails to set any principles for those policies."[79]

2. THE FAIR CREDIT REPORTING ACT (FCRA)[80]

Like the Gramm-Leach Bliley Act, the FCRA applies only to financial institutions that hold or process PII. The Act is "primarily concerned with ensuring [the] credit accuracy" of consumer credit reports.[81] Credit reporting agencies are required to report accurate credit information and to timely correct any false information relating to an individual's credit history. The Act also recognizes consumers' right to access and request correction of any information contained in the consumer's credit report. This right of access and correction is similar to that guaranteed in the E.U.'s Data Privacy Directive. Unlike the Directive, however, the FCRA only applies to information included in individual credit reports.

3. THE IDENTITY THEFT AND ASSUMPTION DETERRENCE ACT[82]

This Act, administered by the Federal Trade Commission (FTC), does not provide any specific protective measures for electronically stored PII. The Act's principal effect is to criminalize (and thereby deter) identity theft activity. While the Act does not afford any specific rights to consumers or impose any obligations on commercial entities, it does empower law enforcement officers to arrest and punish those who seek to criminally exploit PII.

---

[79] Levin & Nicholson, *supra* note 10, at 365.

[80] 15 U.S.C. § 1681.

[81] Levin & Nicholson, *supra* note 10, at 364.

[82] 18 U.S.C. § 1028.

4. TELECOMMUNICATIONS ACT OF 1996[83] AND THE CABLE COMMUNICATIONS POLICY ACT[84]

These two laws, taken together, impose restrictions on the collection and use of PII by entities operating within the telecommunications and cable television industries. Both laws prohibit the collection of PII that is not necessary to perform the relevant contractual service. Any additional collection or use of PII is only allowed in light of the data subject's express consent. In this way, the two laws mirror the notion of "consent before collection" found in both the E.U. and Canada (see below). However, unlike the E.U.'s and Canada's broad legislation, these laws only apply to entities operating within strictly defined industries—another example "of the American piecemeal approach to privacy of personal information."[85]

5. THE CHILDREN'S ON-LINE PRIVACY PROTECTION ACT OF 1998 (COPPA)[86]

COPPA was passed "to protect children's personal information from collection and misuse by commercial websites."[87] Prior to COPPA, it was not uncommon for children's websites to solicit demographical information from minors in exchange for access to online games or content. Congress leapt at the chance to end these unscrupulous practices,[88] and it imposed strict limits on online entities directed at children under the age of thirteen. Specifically, COPPA requires websites soliciting information from minors to "provide parents with notice of their information practices and to obtain parental consent prior to the collection."[89]

---

[83] 47 U.S.C. § 151.

[84] 47 U.S.C. § 551.

[85] Levin & Nicholson, *supra* note 10, at 365.

[86] 15 U.S.C. § 6501.

[87] *Id.* at 367.

[88] What politician wouldn't want to report to his or her constituents that he or she was responsible for legislation aimed at ending the commercial manipulation of children?

[89] Levin & Nicholson, *supra* note 10, at 367.

Like most of the U.S.'s privacy legislation, COPPA is limited in scope: the Act only applies to the collection of PII from children under the age of thirteen.[90] Even then, the law only imposes consent and parental notice requirements.[91] As all of these laws illustrate, the United States has simply failed to mandate broadly applicable uniform standards for the collection, use, and dissemination of electronically stored PII.

C. CANADA

In terms of electronic privacy, "Canadians occupy the middle ground between the E.U. and the U.S., sharing American concerns about 'Big Brother' government, while also having deep concerns about private sector abuse of their personal information."[92] The Canadian Charter of Rights and Freedoms does not explicitly recognize a right to personal privacy,[93] just as the U.S. Constitution does not. Similar to the E.U.'s Data Privacy Directive, however, Canada's national government has implemented widely applicable legislation that restricts the collection, use, and dissemination of electronically stored PII.[94]

Canada's Federal Privacy Commissioner summarized the country's view of privacy as "the right to control access to one's person and information about one's self. The right of privacy means that the individuals get to decide what and how much information to give up, to whom it is given, and for what uses."[95] Thus, Canadians see electronic privacy not necessarily as a fundamental freedom, but as a right to *choose* what PII to reveal and to whom.[96] The following sections explain how Canadian laws reflect this emphasis on freedom of choice.

---

[90] *Id.* § 6501(1).

[91] *Id.* § 6502(b)(1)(A).

[92] Levin & Nicholson, *supra* note 10, at 360.

[93] Lasprogata et al., *supra* note 68, at 6.

[94] *See id.* at 8.

[95] Levin & Nicholson, *supra* note 10, at 392, quoting Privacy Commission of Canada, Speech at the Freedom of Information and Protection of Privacy Conference (June 13, 2002).

[96] *See id.* at 392-93.

1. PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA)[97]

PIPEDA imposes significant restrictions on the collection, use, and dissemination of PII in the private sector. The Canadian national government fully implemented[98] PIPEDA in 2004 with two goals in mind. First, the law was viewed as a "'key lever' in establishing trust and confidence with respect to electronic commerce."[99] Canada recognized early on the need to assure basic levels of privacy in order to facilitate and grow electronic commerce, a point addressed later in this Article.[100]

Second, the Canadian government passed PIPEDA in direct response to the E.U.'s Data Privacy Directive.[101] Canada viewed PIPEDA as essential to guarantee that it met the "adequate" protections required by the Privacy Directive, thereby "[preserving] very important trade relations with the E.U."[102] Accordingly, PIPEDA's restrictions reflect those in the Privacy Directive (although somewhat less severely) in terms of how private entities can collect, use, and disseminate electronically stored PII.

a. COLLECTION

Under PIPEDA, an organization may only collect PII with the data subject's "knowledge *or* consent."[103] This language suggests Canadian entities can collect PII if the data subject is *aware* of the collection but has not necessarily *consented* to the collection. This "either or" provision allows entities to establish "opt out" systems, where PII is

---

[97] Personal Information Protection and Electronic Documents Act (PIPEDA), R.S.C., ch. 5 (2000) (Can.).

[98] The law was originally passed in 2000, and gradually phased-in from 2001 until it was fully implemented in 2004.

[99] Levin & Nicholson, *supra* note 10, at 379.

[100] *See infra* Part III.

[101] Levin & Nicholson, *supra* note 10, at 379.

[102] *Id.* This effort appears to have succeeded. The E.U. now considers it "safe" to transfer electronically stored PII to Canada.

[103] PIPEDA, *supra* note 90, § 7 (emphasis added).

collected unless a user affirmatively elects out of collection. In contrast, the Data Privacy Directive's "unambiguous consent" requirement effectively requires entities to obtain "opt in" consent before they can collect PII. Thus, the Canadian system is more flexible and facilitative of market-based choices than the E.U.'s strict requirements.

PIPEDA also enumerates exceptions to the consent requirement, just as the Data Privacy Directive does. Approved exceptions include situations where collection is "clearly in the interest of the individual and consent cannot be obtained,"[104] when "the information is publicly available,"[105] or when furthering an investigation into "a contravention of the laws."[106]

b. USE

Similar to collecting PII, entities may only *use* PII with the data subject's "knowledge or consent." PIPEDA also restricts the use of PII to purposes for which the data was originally collected, and it limits the ability to keep and store PII to "only as long as necessary to fulfill the purpose for which it was collected."[107] These provisions limit the accumulation of massive amounts of PII in commercial databases, which effectively reduces the chance that a "hacker" or data thief might improperly access and misuse electronically stored PII.

Notably, PIPEDA does not place any sort of restrictions as to *how* an entity uses PII. The law does not, for example, prohibit data-collecting entities from aggregating PII for internal research purposes, or from directing advertisements to PII subjects' home or electronic addresses. Collecting entities are free to make reasonable use of PII, consistent with commercial practices, so long as PII subjects are aware of or have consented to the use. In this way, PIPEDA does not unduly interfere with electronic commerce, and it avoids some of the market distortions that broadly applicable privacy laws might inadvertently produce. Thus, PIPEDA is a fine example of how privacy laws can interact in parallel with a free market system without unduly infringing on marketplace efficiency.

---

[104] *See id.* § 7(1)(a).

[105] *See id.* § 7(1)(d).

[106] *See id.* § 7(1)(b).

[107] Levin & Nicholson, *supra* note 10, at 380.

c. DISSEMINATION

PIPEDA broadly prohibits the disclosure of "personal information without the knowledge or consent of the individual."[108] Similar to the E.U.'s Privacy Directive, PIPEDA provides a list of enumerated exceptions to the "knowledge or consent" requirement. Examples of these exceptions include situations where dissemination is "required to comply with a subpoena or warrant,"[109] when there exists "an emergency that threatens the life, health or security of an individual,"[110] or where otherwise "required by law."[111]

PIPEDA also permits disclosure of PII to certain government entities, much like the Data Privacy Directive. Unlike the Directive, however, PIPEDA does *not* provide a blanket exception to all government agents for any and all purposes. Instead, PIPEDA specifically enumerates the situations under which a commercial entity can disclose PII to a government source. An entity may disclose PII to a government institution, for example, only when the institution "suspects that the information relates to national security, the defence [sic] of Canada," or if the information is needed for "enforcing" or "administering any law of Canada."[112]

Here, again, PIPEDA appears to occupy the middle ground between the E.U. and the U.S. PIPEDA seems to reflect a distrust of government similar to that held by Americans. Rather than allow PII disclosure whenever necessary to pursue a legitimate government interest, Canada has specifically restricted government use of commercially collected PII. This compromise approach—expressly limiting the government's use of PII while acknowledging *some* exceptions—would likely be more palatable to most Americans than the E.U. approach. Thus, PIPEDA again serves as a fine example of how the U.S. could enact broad privacy legislation without issuing the *carte blanche* to government surveillance that Americans fear so dearly.

---

[108] PIPEDA, *supra* note 90, § 7(3).

[109] *See id.* § 7(3)(c).

[110] *See id.* § 7(3)(e).

[111] *See id.* § 7(3)(i).

[112] *See id.* § 7(3)(c.1).

d. REDRESS

PIPEDA offers a strong enforcement provision for privacy violations. Canada employs a Federal Privacy Commissioner charged with ensuring compliance with privacy laws and monitoring any violations.[113] Rather than rely solely on government oversight, however, PIPEDA provides a mechanism by which aggrieved private parties themselves can seek recourse for alleged privacy violations. PIPEDA balances this private remedy with agency oversight in order to limit excessive (and possibly frivolous) lawsuits.

To bring a claim under PIPEDA, a private party files a complaint with the Privacy Commissioner, alleging some violation of PIPEDA. The Commissioner conducts an initial investigation into the complaint, during which time the Commissioner may hold evidentiary hearings or compel relevant parties to produce "any records and things that the Commissioner considers necessary."[114] The Commissioner then files a report (due no later than one year from the date the complaint was filed) that contains any findings, recommendations, and existing settlements.[115]

After receiving the report, the complainant may then "apply to the Court for a hearing in respect of any matter in respect of which the complaint was made."[116] The Court, upon review, might then issue one of several available remedies. The Court might order the organization "to correct its practices" or require the organization to publish notice of any changes the organization voluntarily agreed to make.[117] Finally, in the event of a significant privacy violation, a Court may "award damages to the complainant, including damages for any humiliation that the complainant has suffered."[118]

---

[113] Levin & Nicholson, *supra* note 10, at 379.

[114] PIPEDA, *supra* note 90, § 12(1)(a).

[115] *See id.* § 13(1). The Commissioner is not required to file a report if the Commissioner determines the complaint could "more appropriately be dealt with" through the court system, or if the complaint is found to be "trivial, frivolous or vexatious." *Id.* § 13(2). This interesting mechanism likely relieves some of the bureaucratic pressure that might otherwise impair an agency charged with such a broad task.

[116] *See id.* § 14(1).

[117] *See id.* § 16(a)-(b).

[118] *See id.* § 16(c).

This system of enforcement and redress is interesting for two reasons. First, PIPEDA explicitly empowers a government agency to track compliance and pursue enforcement actions.[119] This ensures entities will not commit minimally offensive privacy violations that, although inconvenient or annoying, would not likely spur a private complaint. Second, PIPEDA allows private parties to hold data-collecting entities accountable while filtering frivolous claims through the Commissioner's office. In doing so, PIPEDA capitalizes on the strength of private parties, who have a strong interest in their own privacy, while minimizing the likelihood of frivolous litigation designed to extort settlements from deep-pocketed defendants. This system seems highly compatible with the U.S.'s approach to private litigation and government oversight. In fact, it might serve as a model for improvement in other areas of the law.

D. SUMMARY

Electronic privacy laws vary greatly from one country to another. When compared to the United States and Canada, the European Union emerges as the most protective of personal privacy. The Data Privacy Directive is a bold, affirmative step towards protecting "personal dignity" in all realms, including electronic commerce. The United States, by contrast, appears reluctant to engage electronic privacy concerns head-on. The U.S has yet to enact a single, comprehensive piece of legislation aimed at protecting electronic privacy in *all* sectors of the economy. Instead, the U.S. continues to rely on a market-based system augmented by occasional (and irregular) legislation. Canada, as others have argued,[120] lies somewhere between the two. PIPEDA marks a "middle of the road" attempt to assuage concerns related to electronic privacy while simultaneously acting to preserve the integrity and efficiency of e-commerce.[121]

Much of the variance between the governing entities is likely attributable to societal norms and traditions. Some cultures

---

[119] Section 15 allows the Commissioner to petition the Court for a hearing even when a private party has not filed a private complaint. Furthermore, § 18 allows the Commissioner to audit, "on reasonable notice and at any reasonable time . . . the personal information management practices of an organization if the Commissioner has reasonable grounds to believe that the organization is contravening [PIPEDA]." *Id.* § 18(1).

[120] *E.g.*, Levin & Nicholson, *supra* note 10.

[121] *See id.* at 379.

undoubtedly value privacy more (and in different realms) than others. To say that one country's laws are "better" than another requires imparting a value judgment on why privacy is important and how much of it is appropriate. This I am unwilling to do. Instead, the following sections attempt to capture the interaction of privacy laws and the "efficiency" of e-commerce in an economic framework. Each country's position on the "privacy-efficiency tradeoff," a concept introduced and explained below, is then approximated. Using the model, I argue that the United States should impose broad privacy protections in order to increase *both* the scale and scope of e-commerce and the level of protection afforded personal privacy.

II. AN ECONOMIC MODEL OF PRIVACY

A. THE MODEL

This Article proposes a new economic framework for analyzing privacy laws, with a focus on electronic privacy and "e-commerce." A fundamental assertion made in this Article (and recognized elsewhere[122]) is that there is an inherent tradeoff between the level of privacy protection afforded to e-consumers and the efficiency of e-commerce. One of the most appealing qualities of e-commerce is the ease and convenience with which a consumer can conduct transactions electronically. "At the most basic level, the Internet makes information flows essentially free, instantaneous, and global."[123] As a government imposes additional safeguards to protect consumers from unscrupulous business practices—such as redundant identity verifications or password entries—the speed and convenience of electronic commerce suffers.[124]

At the same time, consumers no doubt demand a certain level of assurance that their activities conducted electronically, as elsewhere, are afforded a certain degree of privacy. Without a guarantee of privacy at *some* level, it is unlikely consumers would engage in *any* electronic transaction. It is fair to assume, for example, that the explosion of online music purchases through services such as iTunes would not have occurred if Apple had made available to the general

---

[122] *See e.g.*, Whitman, *supra* note 1, at 1192-93; Ciocchetti, *supra* note 3, at 562-68; Fromholz, *supra* note 11.

[123] Swire, *supra* note 2, at 850-51.

[124] *See* Fromholz, *supra* note 11, at 465.

public the names, physical addresses, and purchasing habits of its customers.

There is a tension between the objectives of privacy and efficiency. On the one hand, the absolute absence of privacy protections, whether those protections are regulatory or self-imposed, would significantly reduce the popularity of electronic transactions. On the other hand, an overly burdensome and prohibitive set of privacy laws would almost surely prove too cumbersome for effective e-commerce, and "would lessen or even remove the convenience aspect from Web-based transactions."[125] As one commentator dramatically summarized, "[t]he ability to collect PII from e-consumers allows this ever-expanding economic sector to operate efficiently; serious restrictions on the ability to collect this information is akin to removing a plant from sunlight—e-commerce, as it exists today, would inevitably wither and die."[126] Thus, the world of e-commerce and privacy law, like so many other fields that have consequently suffered the same fate, exhibits a property that readily lends itself to economic analysis: tradeoffs.

1. DEFINING THE RELEVANT TERMS

Because the terms are somewhat amorphous, it is necessary to attach a more specific definition to "privacy" and "efficiency." Here, "privacy" is an index that captures the concerns expressed by e-consumers and the protections designed to assuage those concerns.[127] "Privacy" is used as an index to capture *relative* changes in protections. Any action (such as a widely applicable law) that increases protections on electronic PII will increase the "privacy" index, labeled P_g (where "g" represents a given governing entity, such as the E.U.). Any action that lessens privacy protections will produce a decrease in the privacy index.[128] Thus, "privacy" is used here as an

---

[125] *See* Ciocchetti, *supra* note 3, at 565.

[126] *Id.* at 564.

[127] Here, the term "e-consumers" includes both actual and potential customers who might engage in some sort of electronic transaction involving the exchange of PII. The transaction need not be an exchange of goods or service for money. Accessing a bank statement through a bank's website, for example, would be a "free" electronic transaction involving the exchange of PII (namely, the consumer's user name and password).

[128] This model does not attempt to posit a quantitative cardinal measure of either privacy or efficiency. Rather, these terms are ordinal, and used only to represent *relative* changes. This definition does not affect my argument, however, because I do not attempt to define an "optimum" level of privacy and efficiency. Rather, I argue that an increase in U.S.

ordinal term to assign relative position without assigning a fixed numerical value.

To illustrate: suppose a popular search engine tracks and records all of the search terms originating from a particular IP address.[129] Consumers might be wary of this type of practice, especially if it is done surreptitiously. In response, a government might require all search engines to publicly disclose any recording of search terms in a plainly available "Terms of Use" provision. This government-imposed protection would result in an increase in "privacy."

The term "efficiency" can similarly be defined. For purposes of this model, "efficiency" is an index, E_g, that measures the *scale* and *scope* of e-commerce in a particular government, g. "Efficiency," as it is used here, captures both the *breadth* of electronic transactions and the *number* of those transactions in a governing jurisdiction. Importantly, "efficiency" is not limited to the speed or quickness of electronic commerce (although that is one factor). Rather, it is the overall effectiveness of electronic transactions at serving consumer needs, which in turn is influenced by factors such as speed or quickness.

Any action that promotes the broader use of electronic transactions—say, by opening up new markets to viable Internet commerce—is defined to increase the scope (and thus the efficiency) of e-commerce. Similarly, any action that increases the total number of electronic transactions—say, a new technology that makes authentication more accurate and convenient—will increase the scale (and therefore the efficiency) of e-commerce.

Finally, the model assumes that consumers value both privacy and efficiency. Economically, this means consumers derive positive utility from laws that protect their personal privacy and from the wide availability of e-commerce. Formally:

$$(1)\ Utility = f(Privacy, Efficiency)$$

where

---

electronic privacy protections would result in a net increase in both privacy *and* efficiency. Because consumers value both privacy and efficiency, an increase in privacy protections would therefore create an overall net gain in general welfare. Thus, my argument (i.e., that the U.S. should increase electronic privacy protections) does not require the imposition of an artificial quantitative structure on either variable. A net gain is a net gain, regardless of how large or small.

[129] Indeed, the three most popular search engines—Google, Yahoo!, and MSN (now Bing)—each record PII from user searches. *See* Ciocchetti, *supra* note 3, at 598, 601.

$$(2)\ \frac{\partial Utility}{\partial Privacy} > 0$$

$$(3)\ \frac{\partial Utility}{\partial Efficiency} > 0$$

Of course, Equations (1)–(3) are not meant to suggest there is not a point at which consumers feel there is too much privacy (or too much efficiency); there almost certainly is.[130] But this truth merely reflects the privacy–efficiency tradeoff discussed earlier in this section. Consumers who feel there is too much "privacy" likely feel that way because of the impact excessive privacy protections have on the efficiency of e-commerce, not because they have reached or exceeded a privacy saturation point. If an increase in privacy did not result in added inconvenience and delay, then a consumer would almost certainly desire the additional privacy.

For example, suppose a government required businesses conducting electronic transactions to call a third party clearinghouse (such as a credit reporting bureau) to verify the identity of a potential customer. Such a regulation would delay the speed and increase the direct cost of an electronic transaction, which some consumers would find overly burdensome. At first glance, one might suggest these consumers are suffering from too much electronic privacy. This conclusion is only half-reasoned, however, and false.

These consumers have likely not reached a "satiation point" of privacy. Rather, they are merely at a point where they would prefer to sacrifice some privacy *in exchange for* additional speed and convenience in their electronic transactions. These same consumers would presumably be quite happy with the additional privacy safeguards if there were not a corresponding change in the cost and convenience of e-commerce. The consumers in this example do not suffer from "too much privacy" in the absolute sense; they suffer from too much privacy in the *marginal* sense. They would simply prefer to trade some privacy for increased speed and/or efficiency. Thus, Equations (2) and (3) are consistent with both consumer perceptions and the consumer utility axioms of standard microeconomic theory.[131]

---

[130] *See* Fromholz, *supra* note 11, at 465 ("[A] system that unthinkingly elevates privacy above other interests will give insufficient regard to the costs privacy imposes on the very people it is intended to benefit").

[131] *See generally* HAL VARIAN, INTERMEDIATE MICROECONOMICS: A MODERN APPROACH (5th ed. 1999) (summarizing the axioms of consumer utility theory, including consistency, rationality, transitivity, and non-satiation).

2. THE PRIVACY-EFFICIENCY FRONTIER

As argued earlier,[132] there exists a fundamental tradeoff between privacy protections and the efficiency of electronic transactions. Loosely speaking, that tradeoff can be represented mathematically, where the efficiency of electronic commerce is a function of the level of privacy protections.[133] Formulaically, this relationship can be represented as:

$$(4)\ Efficiency = f(Privacy)$$

where

$$(5)\ \frac{\partial Efficiency}{\partial Privacy} < 0$$

Graphically, this relationship can be represented as a Privacy-Efficiency Frontier ("PEF"):[134]

---

[132] *Supra* Part III.

[133] Again, I am not the first to identify the privacy-efficiency tradeoff. Numerous articles have previously identified and discussed this relationship, at least in the abstract sense. *See e.g.*, Ciocchetti *supra* note 3, at 562-68; Fromholz, *supra* note 11, at 465.

[134] Figure 1 somewhat incorrectly represents the relationship in Equations (4) and (5). Figure 1 portrays "efficiency" as the independent variable and "privacy" as the dependent. This implies changes in e-commerce "efficiency" *cause* changes in privacy protections. This representation is almost surely backwards. As Equations (4) and (5) correctly show, it is far more likely that changes in *privacy* protections cause changes in *efficiency*. Notwithstanding, Figure 1 is more visually intuitive, especially when the "tradeoff threshold" is introduced in the next section. This situation is not unlike that posed by John Marshall's "inverse demand curve," a common (if not notorious) fixture of introductory economic courses.

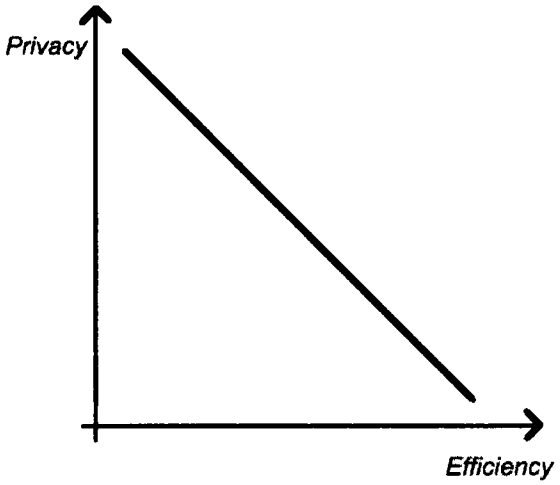

Figure 1: The Privacy-Efficiency Frontier

Note that the PEF models the same tradeoff between privacy and efficiency discussed earlier: for every increase in privacy protections, there will be a decrease in overall efficiency. Likewise, every decrease in privacy measures would increase the efficiency of e-commerce. This relationship, embodied in Equation (5), is intuitive for almost all of the Privacy-Efficiency Frontier. *Almost.*

III. THE TRADEOFF THRESHOLD

Until now, this Article has proceeded from the relatively uncontroversial notion that consumers value both privacy and efficiency in e-commerce, and that there exists a fundamental tradeoff between the two. This section adds a wrinkle to the model. The argument is this: people require a certain base level of privacy before they will engage in electronic transactions. If consumers are not confident their personal information is being protected at some basic level, they might not engage in *any* e-commerce. At some point, the privacy-efficiency tradeoff folds in on itself, and a decrease in privacy protections will lead to a *decrease* in the efficiency of e-commerce.

Suppose a government prohibited all online entities from retaining any user-provided PII. Email service providers and social networking sites, like Gmail and Facebook, would not be allowed to "save" login and password information. Retailers such as Amazon and iTunes would require customers to manually re-enter shipping, payment, and contact information for each individual transaction. As a result,

electronic transactions would be slower and more frustrating, leading some consumers away from e-commerce and back to "traditional" transactions. By eliminating this privacy law, a government would likely expand the scale and scope of electronic transactions (thereby increasing the "efficiency" of e-commerce, as I have defined the term[135]). This action-reaction is entirely consistent with the privacy-efficiency tradeoff captured in Equation (5) and Figure 1.

Suppose, however, the same government eliminated a rule that required online retailers to encrypt databases used to store individual credit card numbers. Or suppose a popular website amended its privacy policy[136] to allow for the sale of PII to third-party marketing companies, who then inundated the data subjects with unwanted emails, phone calls, and pop-up ads. Both of these actions would constitute a decrease in personal data privacy, but neither would likely yield an increase in efficiency. Instead, both of these privacy reductions would likely lead to a *decrease* in the amount of e-commerce, and therefore a *decrease* in efficiency.[137] The argument, then, is that consumers demand a certain basic level of privacy in order to conduct electronic transactions. Short of this level, consumers will not have confidence in the online marketplace, and will eventually take their business elsewhere.

Here, I define this "basic level of privacy" as the "Tradeoff Threshold." At any point below the Tradeoff Threshold, a decrease in privacy protections will lead to an additional *decrease* in efficiency. Graphically, this result is represented by a PEF that "folds in" on itself:

---

[135] *Supra* Part III.

[136] Many of the most popular websites explicitly reserve the right to amend their privacy policy without advance notice. Such amendments are almost always binding, as the consumer's continued use of the site constitutes consent to the new or additional terms. Ciocchetti, *supra* note 3, at 606-08.

[137] Recall that "efficiency" is herein defined as the scale and scope of e-commerce. Thus, any action that leads to a net decrease in the amount of electronic transactions, or that forecloses certain markets from e-commerce, will lead to a decrease in efficiency.

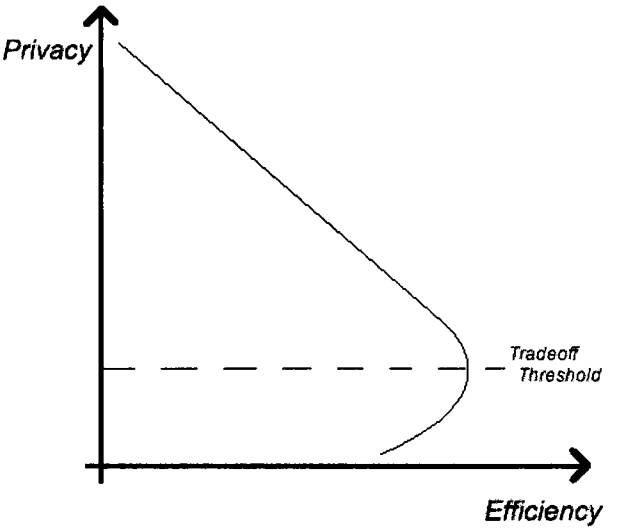

Figure 2: Tradeoff Threshold

Note that the majority of the PEF in Figure 2 (the segment located above the Tradeoff Threshold) correctly reflects the privacy-efficiency tradeoff captured by Equations (4) and (5). However, the points located below the Tradeoff Threshold reflect the argument that the privacy-efficiency tradeoff is not absolute.

Intuitively, this argument is relatively uncontroversial. At some point, people will not engage in electronic transactions if they feel that their personal information is not being adequately protected. Practically, this argument unearths an important policy implication. A country with electronic privacy laws that are located at some point below the Tradeoff Threshold is not bound by the privacy-efficiency tradeoff. A country of this type could increase *both* privacy protections and the efficiency of e-commerce by *increasing* electronic privacy protection laws.[138] Because consumers value both privacy and

[138] An analogy may be drawn here to the concept of Pareto optimality. An allocation of resources is Pareto optimal (or Pareto efficient) if resources cannot be transferred to make one individual "better off" without making another individual "worse off." If resources can be reallocated such that at least one person is better positioned and no person suffers any loss, then the outcome is Pareto sub-optimal, or "Pareto inefficient." *See generally* ANDREU MAS-COLELL ET AL, MICROECONOMIC THEORY 312–16 (1995). The analogy here is not exact. Countries do not "reallocate" units of privacy and efficiency in e-commerce. Nonetheless, the implications on net welfare and "resource" allocation are similar.

efficiency in e-commerce,[139] strengthening electronic privacy laws in this situation would yield a net increase in social welfare *regardless of the social or cultural weight a country affords privacy versus efficiency.*

A. So What?

It would be truly difficult to compare the relative success of privacy laws if the privacy-efficiency tradeoff were constant. Different cultures are defined by different norms, which in turn create different sets of laws designed to protect those norms.[140] To say that one governing entity has a "better" set of privacy laws than another would be to impose the history and culture of one group of people onto an entirely distinct other. To be sure, the E.U. has adopted a stricter set of laws that do more to protect personal privacy than either the United States or Canada. But does that make the E.U.'s system "better" than its North American counterparts? Almost surely not.

A more plausible argument is that the E.U. system protects privacy over efficiency because the European people *value* privacy over efficiency. As one commentator noted, in Europe "the basic issue is of course not just one of market efficiency. [European consumers] need more than credit. They need dignity."[141] The E.U.'s strict system may be optimal given the relative value most Europeans place on privacy (a lot) and economic efficiency (not much). If the U.S.'s free market approach similarly matched the value Americans place on privacy (not much, at least in the commercial sphere) and economic efficiency (quite a bit), then the U.S. system would be optimal *for Americans*. If this were the case, one would have a hard time arguing that U.S. laws are somehow "inferior" to European laws.

But herein lies the rub: If the United States is below the Tradeoff Threshold, then a broad increase in electronic privacy protections would benefit both industry and consumers *regardless* of how Americans weigh privacy versus efficiency. If that is the case, then it is fair—indeed, wise—to take a careful look at how other governments have addressed electronic privacy. The United States might, for example, adopt provisions regarding third-party dissemination that

---

[139] *See* Equations (2) and (3), *supra* Part III.

[140] *See generally* Whitman, *supra* note 1 (discussing how history and culture have influenced privacy laws in the U.S. and Continental Europe).

[141] *Id.* at 1192.

are similar to the E.U.'s or a system of redress similar to Canada's. Either one of these actions might yield a net gain in both privacy and efficiency—*if*, of course, the U.S. is currently below the Tradeoff Threshold. The following section argues that it is.

IV. THE CASE FOR GREATER PROTECTIONS IN THE UNITED STATES

Combining the analysis of international law in Part II and the argument that the U.S. is currently below the Tradeoff Threshold in Part III produces the following image:

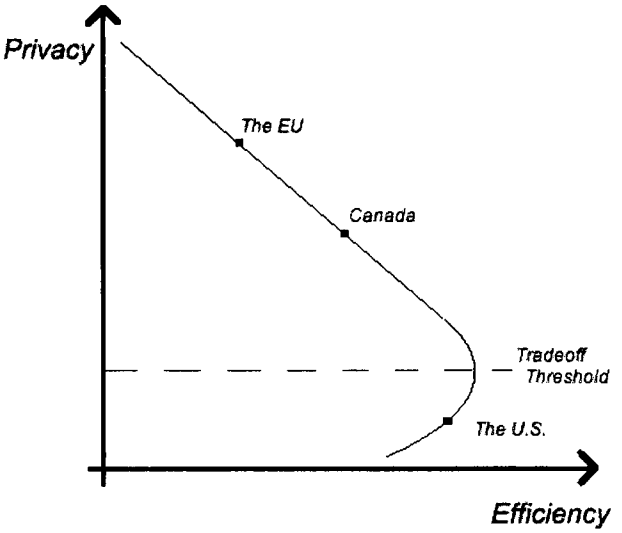

Figure 3: Positions on the Frontier

Figure 3 graphically illustrates the relative positions taken by the U.S., the E.U., and Canada in regard to electronic privacy. As Part I argued, the E.U. has emerged as the most protective of the three, while the U.S. offers the least amount of comprehensive protections. Canada again occupies the middle ground between the two.

The remainder of this Article attempts to justify the argument that the United States is currently operating below the Tradeoff Threshold. That is, that an increase in electronic privacy protections in the U.S. would lead to an increase in *both* personal privacy and the scale and scope ("efficiency") of e-commerce. Part IV.B argues that the current "free market" approach, even when coupled with the patchwork of state and federal legislation, cannot adequately address the concerns raised by electronic privacy. Finally, Part IV.C offers several modest proposals that would push the United States above the Tradeoff

Threshold by increasing privacy protections without a net loss in the "efficiency" of e-commerce.

A. THE UNITED STATES IS CURRENTLY BELOW THE TRADEOFF THRESHOLD

There are at least two arguments suggesting the United States is currently below the Tradeoff Threshold. First, the E.U. continues to classify the U.S.'s privacy laws as "inadequate." This determination forces commercial entities to negotiate specific contracts with European trading partners, which have high transaction costs. Second, the American public has grown increasingly weary of how online entities use PII, a trend that threatens to undermine the continued growth and viability of electronic commerce.

1. CONFLICTS WITH THE EUROPEAN UNION AND THE EFFECTS ON INTERNATIONAL COMMERCE

"[T]he European Union has not found that the overall level of protection in the United States meets European standards."[142] The standoff between the E.U. and U.S. regarding electronic privacy threatens the continued viability of international commerce.[143] As it stands, U.S. companies are forced to negotiate individual contracts with European trading partners or to enter into "safe harbor" agreements. This additional step imposes significant transaction costs on international dealings, and thereby reduces the attractiveness of international commerce.

The recent "safe harbor" agreement brokered between the U.S. and E.U. has done little to assuage the E.U.'s broader concerns. Even with alternative arrangements, "Europeans still constantly complain that Americans do not accept the importance of protecting consumer privacy."[144] Given the high value continental Europeans place on personal privacy,[145] it is unlikely the E.U. will budge on its strict privacy requirements. In the meantime, the continued discrepancy

---

[142] Boyd, *supra* note 10, at 940.

[143] Bloss, *supra* note 45, at 646.

[144] Whitman, *supra* note 1, at 1156.

[145] *Supra* Part II.A.

between the governing bodies "jeopardizes the aspirations of free trade."[146]

2. DOMESTIC RELUCTANCE TO ENGAGE IN E-COMMERCE

Surveys have shown that U.S. consumers are increasingly unwilling to engage in electronic transactions due to growing concerns about electronic privacy.[147] Much of the reluctance appears to flow from consumers' perceptions that "companies collecting their PII are not doing enough."[148] The surveys have at least one lesson to share: online consumers, whether they act on it or not, desire greater assurance that their information is being kept safe.

Comprehensive federal legislation would do much to reassure consumers, arguably in more ways than individual privacy policies (which few consumers actually read, and even fewer understand[149]). Federal legislation would endow consumers with renewed confidence, especially if the legislation assured consumers of redress for privacy violations—something a website's privacy policy is unlikely to do.

B. THE FAILURE OF THE FREE MARKET SOLUTION

The United States has thus far deferred electronic privacy to the free market. Industry leaders have consistently argued that consumers will dictate the appropriate level of privacy protection.[150] If a website does not adequately protect PII, the argument contends, e-consumers will stop visiting it. Over time, the offending website will either be forced to upgrade its privacy protections to "win back" consumer confidence, or it will be forced to shut down. This argument, indeed, is the very same market selection argument that has sustained and perpetuated capitalism as a political-economic ideology for hundreds of years. Why should it not apply to electronic commerce?

Self-regulation in the Internet Age is inadequate for at least two reasons. First, the nature of electronic information precludes the "vote

---

[146] Fromholz, *supra* note 11, at 474, quoting Henry H. Perritt, Jr. and Margaret G. Stewart, *False Alarm?*, 51 FED. COM. L.J. 811, 813-14 (1999).

[147] *See* Ciocchetti, *supra* note 3, at 576-77 (summarizing the survey results).

[148] *Id.* at 577.

[149] *Id.* at 578.

[150] *See* Fromholz, *supra* note 11, at 479-84 (summarizing various "self-regulation" efforts).

with your dollar" power of market capitalism because personally identifiable information, once disclosed, is virtually irretrievable. Suppose a restaurant rendered particularly bad service to a paying customer. The customer, while obliged to pay the bill, would not likely frequent the establishment again. In fact, some customers might make a concerted effort to warn friends and family about the restaurant's inferior service. If the restaurant consistently offered a low quality experience, one would expect it to succumb to its reputation over time and eventually close.

Consider next the typical electronic transaction. A customer, usually alone and in the comfort of his or her home, visits a website seeking some form of a service. The website asks the visitor to submit some personal information—say, a name, email address, and phone number—and the customer obliges. The customer finishes the transaction, closes the browser, and walks away. Suppose the website subsequently sold the PII it collected to a third party marketing company, which then used the information to inundate the consumer with solicitations, "spam" email, and telemarketing. The customer, in all likelihood, would have no idea why he or she was suddenly receiving all of the unwanted attention.[151] Thus, it would be difficult for the customer to say, "I'm not going back to *that* website; they sold me out!"

Furthermore, even if the user were able to correlate the actions with the offending website, there is almost nothing the consumer can do to retrieve the information. When PII "leaves the hand of its collectors and enters the realm of cyberspace . . . it is virtually irretrievable."[152] The same ease and quickness of information transfers that makes e-commerce so appealing also makes it extremely dangerous: "PII is often purchased anonymously and from anywhere in the world. This information can then be resold multiple times until it is completely out of the control of the individual it identifies."[153] Thus, once a customer has suffered through a bad experience, there is very little he or she can do about it. While the restaurant guest might swear never to return and would only lose the cost of the single meal,

---

[151] This is even more likely when there is a significant delay between collection and dissemination. Most collecting websites aggregate PII into "personality profiles" before either using it themselves or selling it to third parties. *See* Ciocchetti, *supra* note 3, at 580. Given the number of websites visited in an average e-consumer's week, it would be truly difficult to relate unwanted solicitations back to any one particular site.

[152] Ciocchetti, *supra* note 3, at 580.

[153] *Id.*

the electronic consumer will continue to be burdened with unwanted e-mail and telephone solicitations.[154]

The second reason self-regulation is inappropriate for electronic privacy involves the growth of electronic commerce. Consumers who have suffered through a bad Internet experience (or who know others who have) will be reluctant to try out new websites. Certain online entities—such as Google, Amazon.com, or eBay—have established a solid reputation for protecting sensitive information. These websites will likely continue to thrive without additional government regulation.

However, *new* websites offering new or improved services face a much tougher battle. Consumers, reluctant to subject themselves to a bad experience, might shy away from untested websites. This is especially true if the website is merely an improvement on an existing idea, and the consumer can complete his or her electronic transaction at a trusted site. This cautious mentality, coupled with the irretrievable nature of electronic data, would effectively quash the very innovation and entrepreneurialism that has and continues to fuel the technology age. Why risk losing your personal information to unscrupulous entities when you can go with the "safe bet," even if the untested website may offer superior service?

New websites, moreover, are not able to effectively combat this start-up signaling problem. A traditional "brick and mortar" business entering a market highly dependent on consumer trust would likely sink hundreds of thousands of dollars into start-up costs to signal their trustworthiness to potential consumers.[155] A new bank, for example, would likely invest in an expensive new building rather than a dilapidated office in a strip mall. A rational consumer would view the up-front investment as a strong signal that the bank is "here to stay," and not likely to run off with suitcases full of money.

Unfortunately, online entities do not have this option. A website is, very literally, a series of letters and symbols strung together and stored on a server. Start-up costs for websites are very low—a fact that spurred explosive growth and innovation in the 1990's but now undermines the stability of new operations. And ironically, it is often

---

[154] Many consumers have reacted to the deluge of unwanted email solicitations by maintaining several email accounts. A consumer might give out one email address to close friends and relatives, and another, infrequently accessed address to businesses and distrusted websites.

[155] Economists often refer to this strategy as "signaling."

the least elaborate web pages that consumers consider the best.[156] Without the usual presence of signals, therefore, it is difficult for new entities to establish themselves as responsible stewards of our most personal information. Together, these failures emphasize the need for new, comprehensive legislation and underscore the disadvantages of continued reliance on market forces and self-regulation. It may prove a tragic irony that those who advocate a market-based approach may be undermining the very market they seek to protect.

C. WHAT CAN WE DO ABOUT IT?

This section offers a few modest proposals for increasing electronic privacy in the U.S. Industry leaders would do well to keep in mind the idea that the U.S. does not need to adopt all or even most of the provisions in the E.U.'s Data Privacy Directive or Canada's PIPEDA. Indeed, the differences between these cultures highly advise against the broad incorporation of any single set of laws.[157] Nonetheless, Americans, as the late movers, have the advantage of examining what has and has not worked well in other countries. The following recommendations are merely the foundations upon which legislators could enact more specific policy provisions.

1. REQUIRE ALL ONLINE ENTITIES TO CLEARLY POST (AND ADHERE TO) PRIVACY POLICIES

First and foremost, the U.S. should require *all* online entities to post privacy policies. This is the least controversial provision, as it only strengthens the current market-based rationale by bridging the information gap between consumers and online entities. "From an information privacy perspective, the biggest problem with the typical e-commerce transaction is that internet users are not fully cognizant of what happens to their PII upon submission."[158] By requiring website operators to post conspicuous links to the entity's privacy policy, the U.S. would at least ensure that consumers are *aware* of how their PII is being used. The FTC itself has recognized notice as the "most fundamental principle" because, "without notice, a consumer

---

[156] Google.com, the world's most popular website as measured by visitors, prides itself on its Spartan appearance.

[157] *See supra* Parts I & II.

[158] Ciocchetti, *supra* note 3, at 560.

cannot make an informed decision as to whether and to what extent to disclose personal information."[159]

2. STRICTLY REGULATE THIRD PARTY DISSEMINATION

Arguably the greatest threat posed by PII disclosure is involuntary dissemination. It is fair to assume that most consumers are willing to share their information with an entity that collects it, so long as the collection is conspicuous and the consumer has chosen to voluntarily reveal the information to the site. This reflects the consumer's judgment that the website is trustworthy, which is a finding legislators should respect.

If "trustworthy" websites are then free to disseminate that information to other sources, however, the consumer's reasoned judgment is completely undermined. Consumers, and often data-distributing entities, simply do not know who is buying the information and what they are doing with it.[160] Industry leaders certainly have a fair argument when they claim that PII use and collection is purely voluntary and controlled by the consumer. It most often is. However, industry leaders appear unwilling to (and likely cannot) guarantee the safety of any PII disseminated to a third party. Instead, companies often have "systemic incentives to overuse personal information where customers have imperfect information about privacy practices and thus will not find out about abuses."[161] By adopting federal legislation or regulation that restricts dissemination of PII, the U.S. would undercut this "systemic incentive."

The effectiveness of such regulation hinges, of course, on the ability to track the distributed information and to punish those who improperly release it to third parties (something I have argued is difficult to do). There is, however, at least one cheap and simple solution: the FTC or other regulating entity could "test" online entities by creating false information profiles and releasing them to single, isolated entities. Because the information would only be released to a single entity, any future dissemination (and subsequent use) of that information could be traced back to the original entity.

---

[159] FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf (last visited March 2, 2011).

[160] Ciocchetti, *supra* note 3, at 580.

[161] Boyd, *supra* note 10, at 945.

Suppose, for example, a regulating entity created a fictitious information profile complete with a new email address (account_12345@gmail.com) and personal information (age, occupation, and physical address). The regulator could then use the information to register for services offered through a target website. Aside from this initial disclosure, the regulating entity would not release or reveal the information to any other entity. If the regulator received any unsolicited emails making use of the profile, the regulator could investigate the target entity and potentially impose some form of sanctions. Perhaps the most attractive feature of this option is its low cost: many providers offer free email registration, and a single regulatory agent could monitor thousands of "test profiles" at a time.

This approach is, of course, unlikely to track all improper dissemination, just as an undercover DEA agent is unlikely to catch all drug traffickers. Nonetheless, a broad prohibition on improper dissemination of PII—coupled with an enforcement mechanism, weak as it may be—would at the least achieve an expressive and deterrent effect into the market for electronically-stored PII. Furthermore, the regulating entity could target its efforts toward large websites that collect significant amounts of PII. And while it may be unlikely that a new federal law would "scare" all unscrupulous entities into ceasing all unauthorized distribution of PII, it is even less likely that a single one of those entities would cease distribution without such a law.

3. NEGOTIATE WITH THE E.U. TO OBTAIN "ADEQUATE" STATUS

The U.S. needs to negotiate some compromise agreement with the E.U. in order to protect valuable trade interests. The Data Privacy Directive is not a machine. It was implemented and still is operated by humans. The U.S. does not *necessarily* need to comply with every letter of the Directive. Rather, they simply need to convince the E.U. that the U.S. affords "adequate" protection. This nebulous definition leaves plenty of room for negotiation, meaning the U.S. does not necessarily need to sacrifice its own views and values simply to comport with the E.U.'s.

As Canada's PIPEDA attests,[162] a country need not wholesale adopt the Data Privacy Directive to achieve "adequate" status. PIPEDA represents a compromise between the Canadian government and the E.U. On many levels, the E.U. would surely prefer the United

---

[162] *Supra* Part II.C.

States obtain "adequate" status—transaction costs are, after all, built into the eventual price of a deal, and both parties are affected by that price. The Canadian experience suggests the E.U. would work with the United States to form a mutually agreeable covenant that would provide the assurance and protection the E.U. desires without completely infringing upon the United States' conception of privacy and commerce. Just as the Canadian government has integrated its own views of personal privacy and the value of commercial efficiency into PIPEDA, the United States, as an extremely valuable ally of the E.U. (both economically and politically), can surely do the same.

CONCLUSION

The persistent evolution of technology and the growth of e-commerce will continue to threaten personal privacy. Any rule structure that seeks to protect electronically stored PII in the face of this threat must be careful not to afford "insufficient regard to the costs privacy imposes on the very people it is intended to benefit."[163] Privacy protections, it has been argued, may come at the expense of the very speed and convenience that fuel e-commerce. The "optimal balance" of privacy and efficiency depends greatly on the historical and social norms of a given people. A system that works well for one group does not necessarily meet the needs of another.

However, the privacy-efficiency tradeoff is not constant. At some point, the lack of adequate privacy protection *decreases* the scale and scope of e-commerce. Without a basic level of privacy protection, consumers will be reluctant to engage in electronic transactions for fear that the online entity will use their information in unwanted ways. This fear rings especially true with new and untested online entities, the success of which is key to further innovation and growth in the industry. A governing entity that finds itself below this basic level of privacy protection would increase both privacy and efficiency if it instituted greater privacy protections and thereby increased consumers' confidence in electronic transactions. This is true *regardless* of the relative value a particular society places on privacy and efficiency.

The United States is one such entity whose privacy protections are below the basic level. U.S. privacy laws are spotty at best and hinder electronic commerce at worst. The lack of uniform privacy protections in the U.S. forces commercial entities to form specific privacy

---

[163] Fromholz, *supra* note 11, at 465.

agreements with European trade partners, which are high in transaction costs. American companies are also forced to comply with a patchwork of rapidly changing laws. And most importantly, the lack of privacy protections threatens to undermine consumer confidence in electronic transactions and stifle growth in the nation's most promising new marketplace.

By mandating widely applicable privacy laws that, at a minimum, require notice and/or consent before collecting PII, the U.S. would benefit from a net increase in consumer welfare. In the end, consumers and commercial entities alike—both foreign and abroad—would reap the benefits of a reassured marketplace subject to uniform restrictions and predictable standards. Industry leaders should abandon their staunch reliance on self-regulation, and instead work with lawmakers to design a new paradigm of privacy laws that best fits the wants and needs of the American consumer. "[L]egal protections," after all, "play an important role as consumers choose how to conduct their online transactions. . . . Law, rather than being an enemy of the market, is a facilitator of it."[164]

[164] Swire, *supra* note 2, at 860.